

The Essential Guide to Online Safety



This is serious



ONS:

“There were **4.1 million** reported offences of fraud in 2024.
A **33% increase** from 2023”



The National Crime Agency:

“...we estimate only **14%** of fraud cases are being reported”

National Audit Office:

“Online fraud is now the most commonly experienced crime... it has been overlooked by law enforcement...”



Action Fraud:

“**80%** of all fraud is on the internet”



Action Fraud:

“Surrey & Sussex Police were sent **5600 reports** of fraud in 2023.
This resulted in **259 prosecutions**” (4.6%)

FOI requests to the police revealed:

Surrey: **2357 officers** employed. **11** are on the ‘Fraud Desk’ (<0.5%)
Metropolitan: **34,328 officers** employed. **245** are on the ‘Fraud Desk’ (0.7%)



House of Commons Justice Committee:

“**2 per cent** of police funding is dedicated to combating fraud but
it makes up **40 per cent of reported crimes**”.





Passwords



Password strength:

LondoN2018 19Evelyn82

Mix of lower & upper case and a few numbers
Barely adequate but are easy to remember

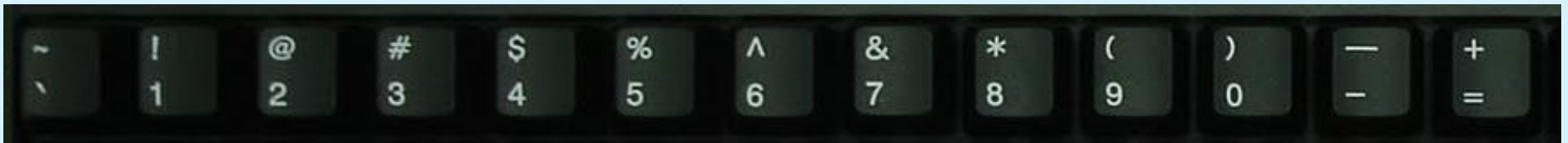
Tp4Z\$rT5q1i9s&3z5c2iD

Great password but difficult to remember!

Passwords

Better passwords:

Use 'odd' characters from the keyboard –



These improve password strength

Passwords


Good to use different passwords for different places –
but difficult to remember them all

Use a few passwords

Use more complex passwords for important websites

(Websites that don't store your personal details could all have the same password.

Examples - BBC, newspapers, e-card sites, DIY stores etc)

The  recommend you do **NOT** change your password
regularly

(But do change it if you think it's been compromised)

Passwords

Good Passwords – that you can remember:

Use an acronym that means something to you.

My daughter's birth date is 13 April 1982

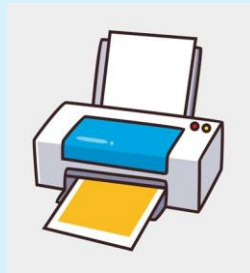
Can become: **Md'sbd13Apr82**

or

Use three random words

Example:

Fruitbowl.Wardrobe.Printer



Passwords

Don't use:

Something that you might refer to in a conversation
(Partners / child's / grandchild's name, favourite sports team,
street where you live, pet's name etc)

Do use:

Something that doesn't come up in conversation:
(Mother's place of birth, partner's middle name, father's first name etc)

Consider:

A Password Manager - 'ProtonPass' 'Nordpass' '1Password' etc
(Search for 'password manager')

Passwords

**Don't forget your
mobile phone!**

Most are purchased with
no password set

(Use fingerprint / facial recognition if available)



Passwords

Whatever password you choose, find out how good it is at

passwordmonster.com

A password based on your grandson's name and birth year doesn't take long to break

How Secure is Your Password?

Take the Password Test

Tip: Don't simply change e's for 3's, a's for 4's etc. These are well-established password tricks which any hacker will be familiar with Show password:

George+2018

Very Weak

11 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
18.09 seconds

Fruitbowl.Wardrobe.Printer

Very Strong

s containing: Lower case Upper case Numbers

Time to crack your password:
4 million years

These passwords take a bit longer

Md'sbd13April82

Very Strong

s containing: Lower case Upper case Number

Time to crack your password:
29 million years

Passwords – a final word

Two Step Authorisation (2SA)

Also known as **Two Factor Authorisation (2FA)**

Adds a second layer of security –
in addition to your password



If it's an option – enable it



The website sends a code - usually via text - that you have to enter before you can finish signing in.

Turn on 2-Step Verification

Bank Accounts



You can reclaim any money lost as long as you haven't displayed "Gross negligence"

Bank security is probably perfect



So – scammers try to trick *you* into giving them your details

Phishing

Maybe like this:

[PayPal](#)

Because it has expired, your credit card has been removed from your PayPal account.

If this was the only credit card on your PayPal account, you will need to add a new card to continue sending instant PayPal payments.

To add a new debit or credit card, log in to your PayPal account at www.paypal.co.uk, go to your Profile, and click **[My money](#)**.

Yours sincerely,
PayPal Direct

If you clicked on the link...

You'd arrive here...

Phishing



Looks good, but this is a web forgery

But you thought you were here

Phishing

PayPal, Inc. (US) https://www.paypal.com/uk/cgi-bin/webscr?cmd=_login-run&dispatch=5885d80a13c0db1f8e263663d3faee8d4026841ac68a446f69dad17fb2afeca3

Confirm Information. - Spam - 'Ya... x Login - PayPal x Login - PayPal x +

Sign Up | Log In Search

PayPal

Home Personal Business Safety Advice Where Can I Shop? Help

Homepage Why PayPal? Using PayPal Managing Your Account Send Money

Account login

Email address

PayPal password

Go to

[Problem with login?](#)

New to PayPal? [Sign up](#)

GET EXCLUSIVE DISCOUNTS FROM LEADING RETAILERS WHEN YOU SHOP WITH PAYPAL

Shop now at www.paypal-shopping.co.uk

terms and conditions apply

[About](#) | [Account Types](#) | [Fees](#) | [Privacy](#) | [Safety Advice](#) | [Contact Us](#) | [Legal Agreements](#) | [Developers](#)

VeriSign Identity Protection

This is the genuine web site

Phishing



Look at the real website address

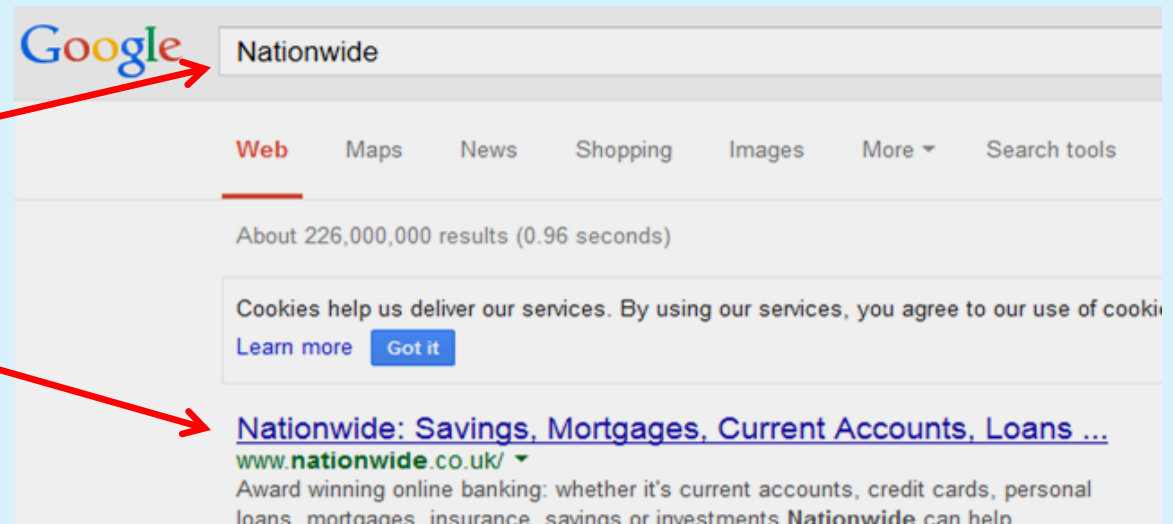


It is safest to type in the web address yourself



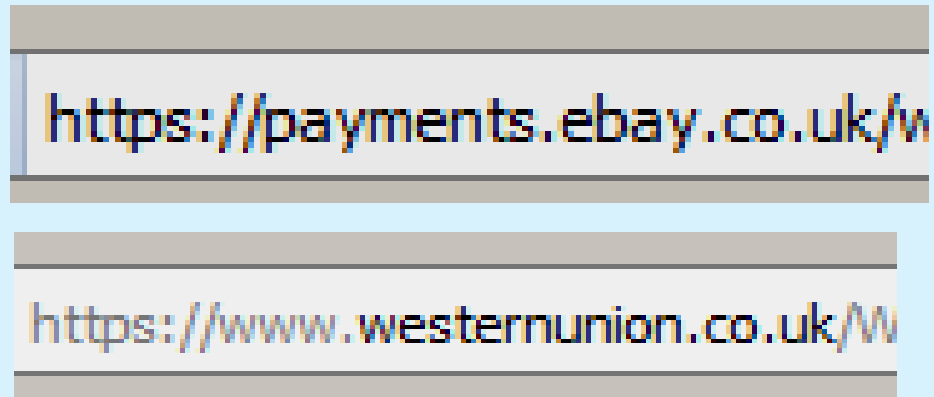
Or carry out your own web-search...

and follow the link

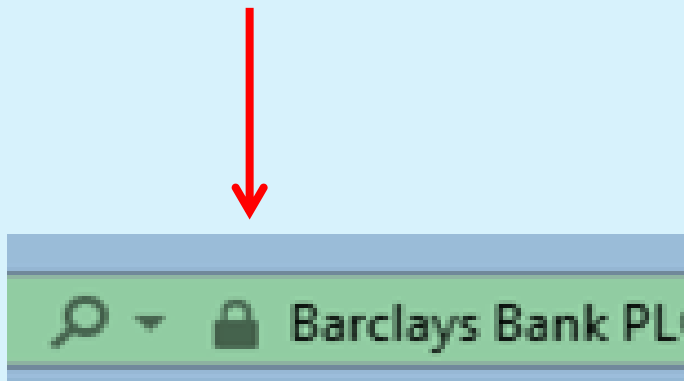


Using Money Online

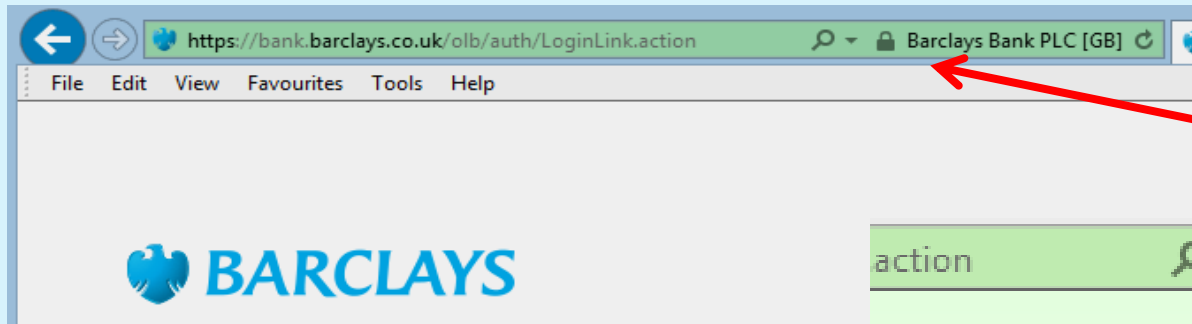
Https means your data cannot be intercepted. But it doesn't mean it is a **trustworthy** site



The small padlock is not a guarantee that the site is trustworthy



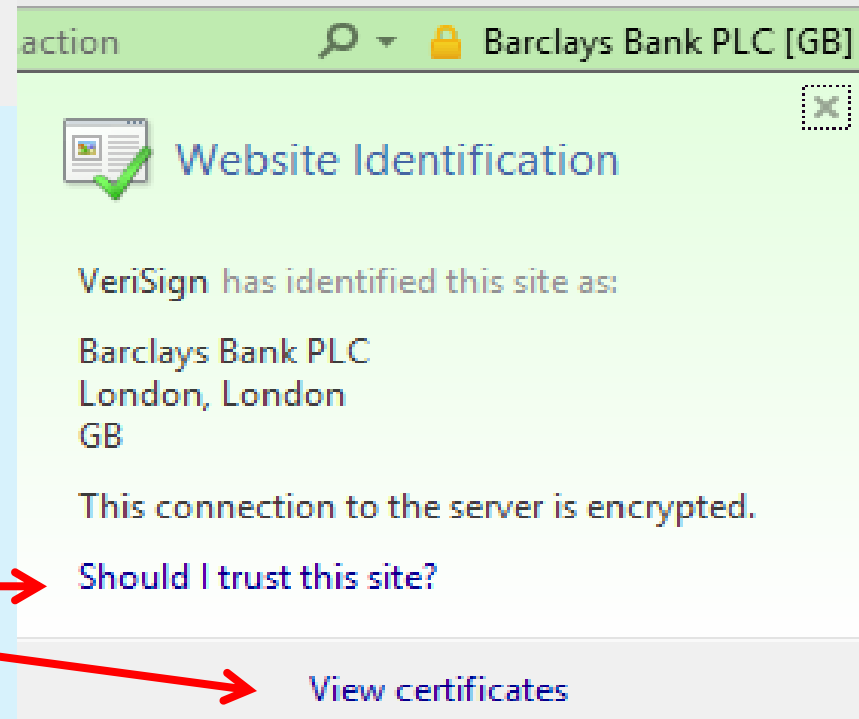
Using Money Online



Click on the padlock....

You will see more information – check the details

And follow the links for more detailed information



It should give you confidence that it is a genuine site

Using Money Online

Use a credit card instead if you can.
The seller won't know your bank details
and the card company will have a
method of dispute resolution

For an extra layer of security:

Sign up to an online payment
platform:

PayPal / Apple Pay / Google Pay

Use it to pay the supplier, if it's an
option



Sign up

Country or region
United Kingdom

Your email address

Create your PayPal password

Add and confirm your phone number

Code
+44

Phone number

Next

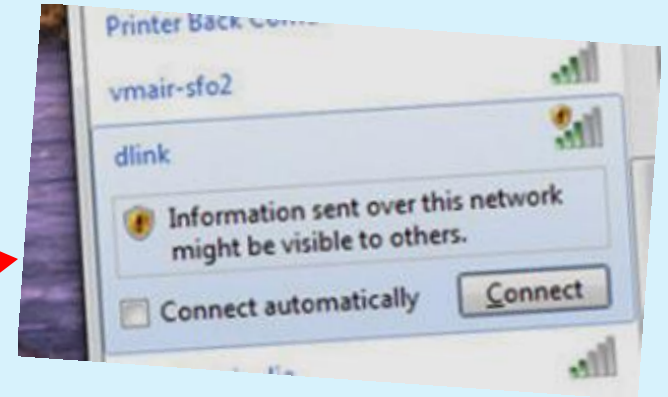
It puts a trustworthy agent between
you and the supplier

They all have a dispute resolution
centre



Public Wifi

Public internet access is inherently unsafe



A hacker can access your device if they are using the same router

If you use public WiFi, **never** do anything confidential or use a debit or credit card



Safer Internet Browsing

We've all heard of service providers being hacked

Maybe your data was stolen...

Co-op cyber attack affects customer data, firm admits, after hackers contact BBC



M&S reveals hackers accessed customer data

MARKS AND SPENCER | CONSUMER | CYBER ATTACK | Tuesday 13 May 2025 at 8:11pm

NEWS

POLITICS

FOOTBALL

CELEBS

TV

SHOPPING

ROYALS

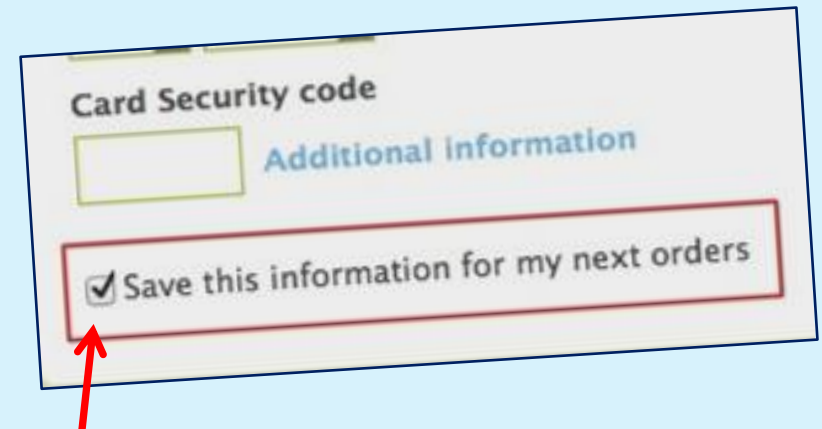
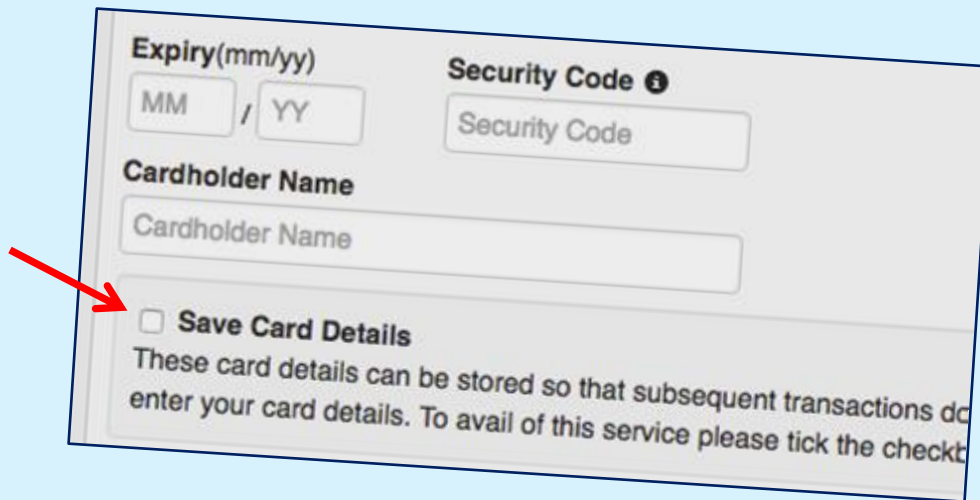
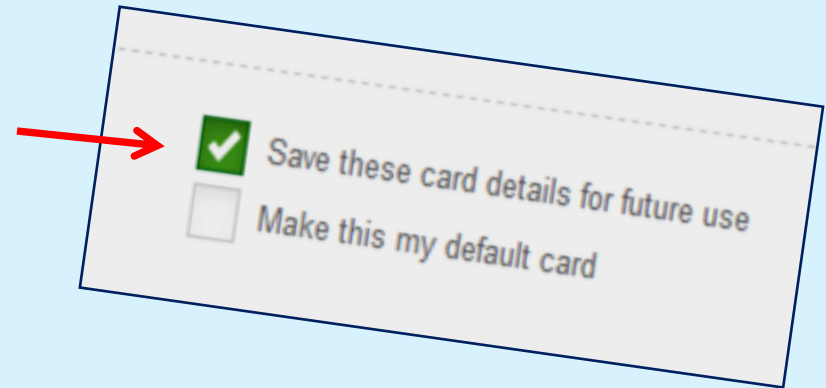
Harrods cyber attack: Luxury store is latest target in worrying trend

Harrods follows M&S and the Co-op in being targeted by cyber hackers in recent days, with the other two supermarkets still reeling days after the attacks which caused chaos

Safer Internet Browsing

It is not quite as convenient, But if you **don't** allow the provider to store your card details, you'll be less exposed

Make sure the 'Save' box is **not** ticked



After a data breach, be **very** suspicious of any emails asking you to 'confirm your details' or reset your password

Has your data been stolen?

Visit

haveibeenpwned.com

Enter your email address into the box and click on 'pwned?'

';--have i been pwned?

Check if your email address is in a data breach

xxxxxx@yahoo.co.uk

pwned?

[Using Have I Been Pwned is subject to the terms of use](#)

Has your data been stolen?

haveibeenpwned.com

If you see this message -

You need to change the password on that account

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the breaches that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing your password.



Nitro: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Names, Passwords



Twitter (200M): In early 2023, over 200M records scraped from Twitter appeared on a popular hacking forum. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to Twitter profiles. The subsequent results were then composed into a corpus of data containing email addresses alongside public Twitter profile information including names, usernames and follower counts.

Compromised data: Email addresses, Names, Social media profiles, Usernames

Email Scams

Scam emails are better than they were

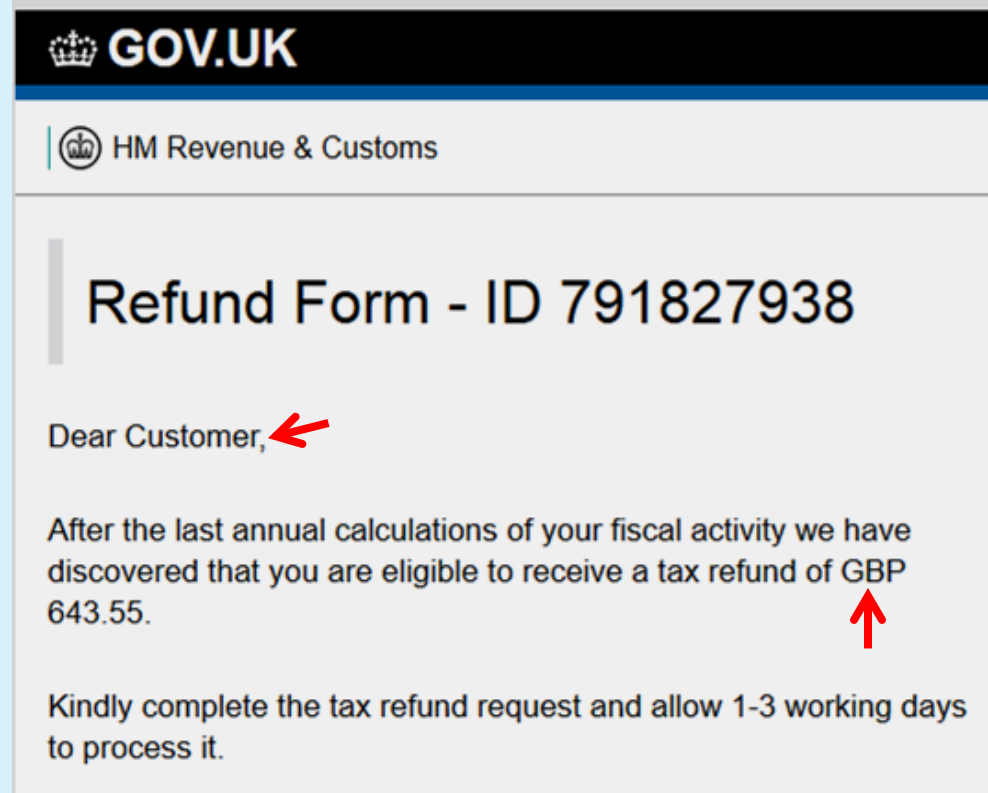
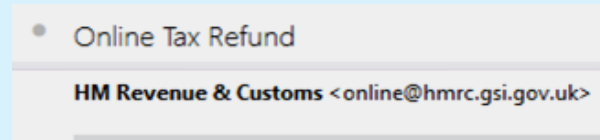
It has a genuine looking email address

Correct logo

No spelling or grammar mistakes

A believable £643.55

BUT: Not addressed to you and no '£' sign

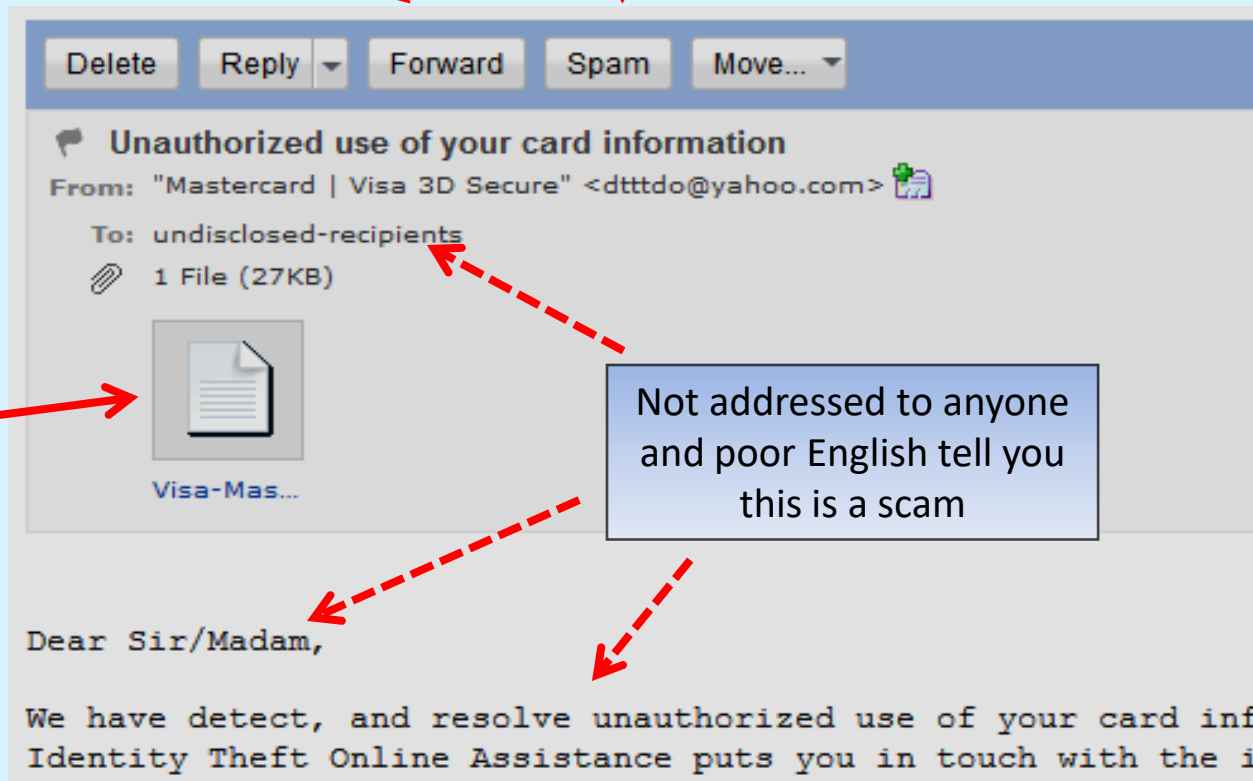


Email Scams

Forward this to report@phishing.gov.uk and the National Cyber Security Centre (ncsc.gov.uk) will try to get the sender shut down

Then click on 'Spam'. This email will be sent to your Spam folder

All future emails from this address will bypass your 'In' box and sent straight to the spam folder



And...

Never reply or 'unsubscribe' as you just confirm your email address is active

Email is Not Secure

Why does your bank never email statements to you?

Because email is not secure

You might log-on to an https website, but the email will be forwarded on to many computers during it's journey

It *travels in plain text* over the network and will be *stored in plain text* on email servers

Think of your email as a postcard!

For a secure email, search for: Proton Mail, Startmail, Tutanota, Zohomail or Thexyz



<https://mail.google.com/>

<https://mail.yahoo.com/>

Google have said they have (now) stopped reading emails for keywords to show more personalised adverts



Text & Phone Scams

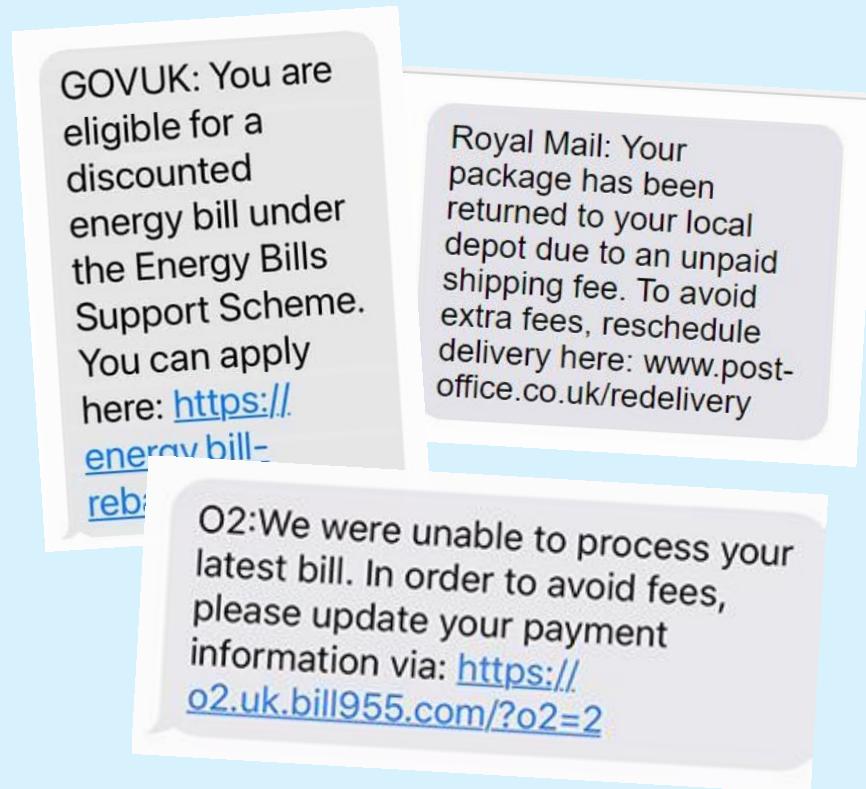
If you receive a phishing / scam text, NEVER respond.

Forward them **7726** and the National Cyber Security Centre will get the sender shut down.

(**7726** spells SPAM on an alphanumeric keypad)

If you receive a phone call claiming to be from your bank or building society, hang up and phone **159**

<https://stopscamsuk.org.uk/159>



Social Media Safety



Use extra precautions when using social media on mobile devices

Don't:

- Tweet photos from inside your home
- Mention your address on any social network
- Announce when you're going on holiday
- Post your holiday pictures whilst on holiday
- Post photos of new expensive items you've bought or received
- Assume the safety settings of your social profiles are where you left them

According to the Surrey Police...



The Essential Guide to On-line Safety



For further study, the following websites are recommended:

actionfraud.police.uk

cyberaware.gov.uk

getsafeonline.org

thinkuknow.co.uk

thinkjessica.com

bbc.co.uk/webwise

welivesecurity.com

takefive-stopfraud.org.uk

ncsc.gov.uk

disney.co.uk/internet-safety



Be secure when you explore

Don't forget your bank or building society will have their own security pages!



The Essential Guide to Online Safety – the last slide!

I hope this presentation has been useful

A pdf version of these slides
is available at

<https://tinyurl.com/5bmm6x5z>

Or use:



Any feedback (good or bad) is gratefully received at:

presentationfeedback2023@gmail.com

Thank you in advance!